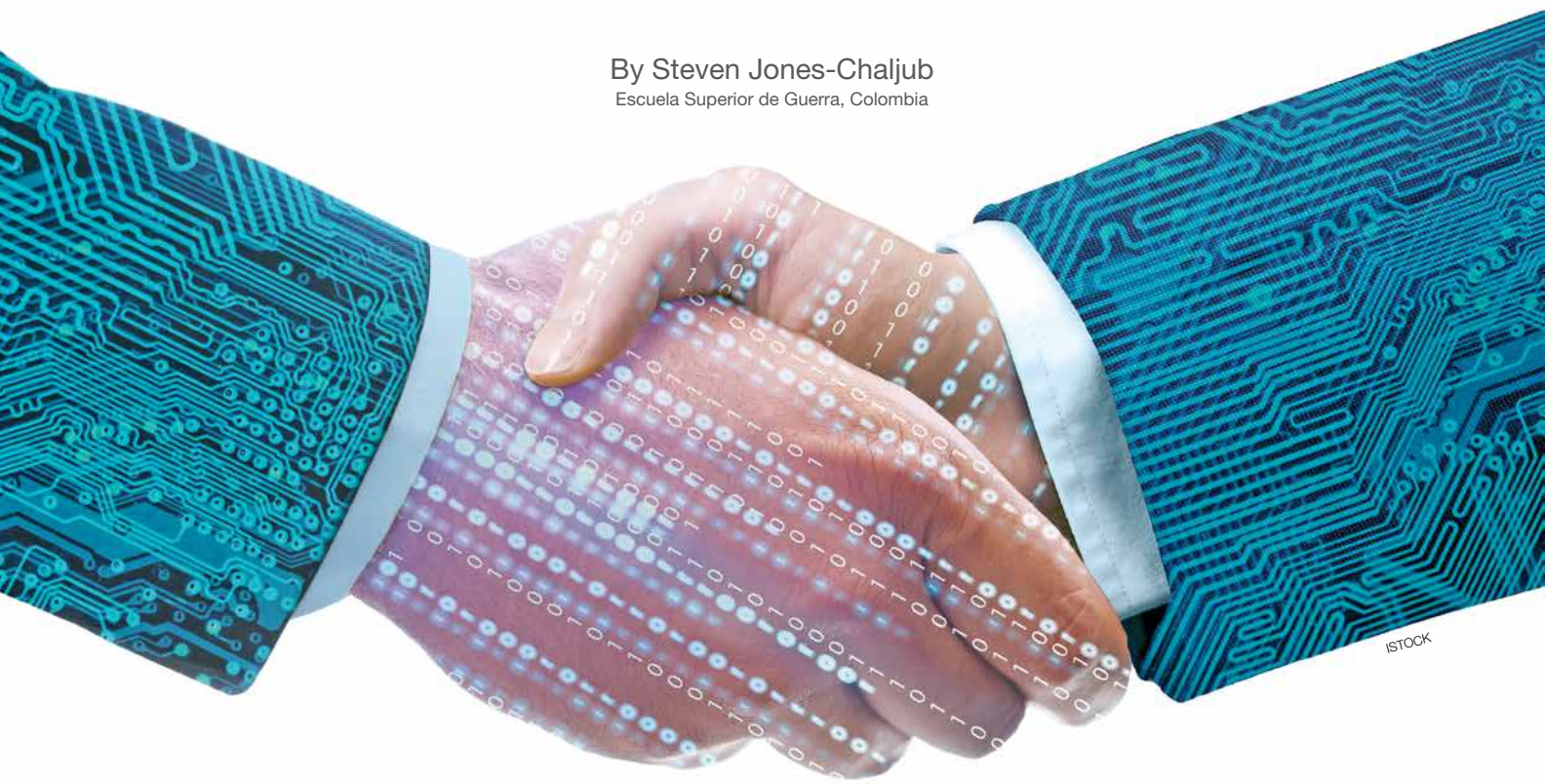
BUILDING TRUST TO FIGHT CYBER CRIME

RELIABLE REPUTATION ONLINE IMPEDES CYBER CRIMINALS

By Steven Jones-Chaljub
Escuela Superior de Guerra, Colombia



ISTOCK

Cyberspace is a dynamic domain that attracts attention from academics and policymakers. It represents the present and future of our societies. Cyberspace has hundreds of definitions and most include a human component that cannot be ignored. People shape cyberspace, demanding and creating more ways to interact with each other in "virtual communities." Within virtual communities, the sociological variables required for community building are present: rules, rights, duties, membership, authority and trust.

Trust is especially important for cyberspace to work; however, the anonymity characteristic of this domain creates important challenges. To build trust, virtual communities have relied heavily on reputation, under the premise that a better reputation equals more trust and, therefore, greater interaction.

Cyberspace is not entirely safe; it challenges the security of people and systems. Cyber crime, in most of its modalities, requires the victim's voluntary or tacit cooperation to work. Cyber crime exploits the trust that individuals have in the system, other people, or both. Cyber crime has a psychological modus operandi and requires the same type of response.

THE IMPORTANCE OF TRUST

The decisions people make shape cyberspace in size and nature, giving constant birth to opportunities and threats. This ever-changing domain lets users interact despite great distances and without previous relationships.

Cyberspace has given birth to unexpected social phenomena; for instance, it has blurred the line between real and cyber life. Aristotle once said that humans are social animals. Thousands of years later, this is still true. Users have created communities in cyberspace for every purpose. Scholars of social sciences are now studying these "virtual communities" to better understand online social interactions. These studies indicate that, although there is no consensus on governing cyberspace as a whole, its virtual communities are not entirely anarchical.

Virtual communities are full of rules and hierarchies that, through membership, grant benefits and impose duties. Membership is discriminatory, as stated by Phillip Cole, in his 2012 article, "Taking Moral Equality Seriously: Egalitarianism and Immigration Controls," and Michael Walzer, in his book, *Spheres of Justice: A Defense of Pluralism and Equality*. It creates a distinction between insiders and outsiders, in which insiders are perceived as those driven by the desire for a common idea of life, and outsiders as a disruptive force. Therefore, virtual communities cannot exist without membership, and people have the right to impose limits on it to protect their "common ideal." Walzer describes membership as a good distributed by the community because it is perceived to have certain value; for instance, it grants trustworthiness to insiders.

As there are benefits of membership, there are also rules to protect the community, which require an authority that exercises control. Virtual communities have control mechanisms tailored to their needs. Online vigilantes, administrators and system providers enforce the rules and penalize deviant behavior with prescribed punishments, such as suspension, account deactivation or law enforcement reporting.

Virtual communities have a unique characteristic: becoming a member does not require social scrutiny. In traditional human interaction, individuals wishing to become part of a community have had prior contact with established members; however, in virtual communities this is the exception. An individual can become a member of a virtual community simply by joining, a process that may only require creating a profile and authenticating identity. For example, by creating an account on eBay or Amazon, individuals are members and can interact with each other. This exerts pressure on the relationship between membership and trustworthiness, because the first is no guarantee of the latter. Thus, members of virtual communities must consider two questions: Is the other a true member? And, if so, can they be trusted?

Trust is everything in cyberspace because it keeps relationships between individuals and different systems running smoothly. Nonetheless, building trust is a challenge, given anonymity and lack of physical contact. To

satisfy this deficiency, virtual communities rely heavily on "reputation." Reputation becomes the most valuable asset for individuals seeking to access the benefits granted by a virtual community. For instance, buyers and providers in e-commerce (e.g., eBay, Amazon, Craigslist), service platforms (e.g., Uber, Airbnb, Booking) and online games (e.g., Second Life, World of Warcraft, League of Legends) constantly evaluate each other's reputations. The higher your profile's reputation, the more trustworthy you will be perceived, making it easier to have successful interactions and access to more information. It has reached the point where specific scams are created just to build reputation within a virtual community (e.g., Amazon reputation scam).

Trust through reputation can be earned by different means. Complying with the rules, being recognized as competent, having members of high reputation that can guarantee your own and achieving positive feedback all build the perception of trustworthiness within virtual communities. However, persistence and patience are necessary to avoid the appearance of opportunism. For example, within blogs, only those individuals with a good reputation are trusted with the highest roles (i.e., administrator, editor) that grant important privileges that, if used incorrectly, could jeopardize the entire community.

In cyberspace, trust is required not only of individuals within virtual communities, but also of the systems that support those communities. A reliable system must be able to successfully support social interactions, without greater setbacks in accessibility and governability. Trust in the system affects members' "stickiness," that is, their willingness to stay and use the platform. Thus, stickiness has a correlation with revenue realized by the system's owner. Fewer people using the system equates to less traffic, fewer transactions and, therefore, less money and less influence on the internet.

TRUST AS A DENIAL MECHANISM

Cyber crime has a characteristic that is hard to find elsewhere: the victim's voluntary or tacit cooperation. Tactics such as phishing, smishing, credit card farming, key-logging, bot-net building and identity stealing require, at their early stages, action from the victim to work. Cyber victims are not compelled to act, yet do so because — ignorant of the others' intentions — they trust the concealed cyber criminal, the system, or both. Cyber criminals exploit such trust and ignorance and trick their victims into making the required "click," plugging in infected hardware, making advance payments or disclosing personal information. They also rely on the private information that their future victims recklessly disclose in virtual communities perceived as safe (e.g., travel documents and forms of identification posted in social networks).

Trust pushes people to implicitly cooperate with cyber criminals, and that cooperation is mandatory in the early stages of most cyber tactics. Examples are the Nigerian letter scam and Stuxnet. In the letter scam, an email depicting a reliable source (e.g., the United Kingdom lottery, the FBI, the U.S. Marine Corps, Microsoft) requests private information or payments. According to the Australian government platform ScamWatch, in 2015 this scam affected at least 980 people, resulting in financial losses of AUD $4.5 million in Australia alone. Email was the delivery method in 56.3 percent of instances. Stuxnet, on the other hand, a highly elaborate malware intended to affect Supervisory Control and Data Acquisition systems, infected an Iranian uranium enrichment plant in a classic social engineering attack via USB sticks.

The relationship between membership and trust in virtual communities, and the fact that such communities are not anarchical, indicates that reputation can be enhanced as a tool to deny cyber criminals' access to potential victims. Because reputation is mandatory for trust-building in cyberspace, a lack of trust means it is unlikely that individuals would cooperate with their cyber victimizers. Therefore, without reputation there is less interaction and collaboration, and without the victim's cooperation, many cyber crime tactics are useless.

There is evidence that trust built through reputation effectively hinders cyber criminals and cyber scammers. Posts in various virtual communities — ranging from E-Trade to online gaming sites — associate scammers with members who have poor or no feedback and suggest a minimal reputation threshold as a criterion of trustworthiness and eligibility to participate in the community. While such mechanisms are not foolproof, they impose obstacles.

Reputation is an obstacle for cyber criminals because it limits interaction with potential victims and its effect cannot be overcome. Achieving trust through reputation requires time, and it is unlikely that criminals will invest much for a limited

SAMPLE BLOG POSTS ILLUSTRATE THE IMPORTANCE OF REPUTATION IN BUILDING TRUST ONLINE.

Blog: Amazon Daily Forum
Date: Jul 2, 2012 9:38:41 AM PDT
User: J_Onyx
Message: "As a rule, I don't buy from Marketplace Sellers. When I have no other reasonable alternative, I check out the seller. If I do not like what I find (too high a risk), I consider the amount of money involved. For instance, under no circumstances will I order anything that costs more than $10 from a 'new' seller."

Blog: Ebay's Community
Date: August 11, 2009
User: baby_keanu_vintage
Message: "Listen to me, when I say: 'Do not sell to "zero" feedback bidders!' Why? Ebay is a shark tank. Competitors will open phantom accounts and bid way over the market price to steer traffic to their own listings! It's a complete waste of your time if the bidder doesn't pay! You will have to wait one week to file a claim and wait another week to get the FVC (final value credit). When all is said and done...the market price may have dropped by the time you finally do sell it. What to do? Sell only to bidders with at least three verifiable feedbacks."

Blog: Steam User's Forum
Date: 03-04-2015, 06:34 PM
User: Smegmadeus
Message: "Surely something can be done to stop these scammers? It's been going on long enough. How about adding a bit of protection to steam accounts to stop this happening. It wouldn't be too difficult to add some account options: e.g. don't accept invites from players with private profiles and, don't accept invites from zero rank players."

An employee at the elite Bretagne-Sud cyber security center in Vannes, France, simulates a cyber attack. AFP/GETTY IMAGES

number of attacks. Consistent deviant behavior leads to isolation from the community and ultimately to profile blacklisting or suspension. Instead, most cyber criminals prefer targets of opportunity and "fishing-net" logic: Hit as many small victims as possible in a short time and without any distinction. This partly explains why a single scammer often has multiple accounts within a virtual community.

System providers also use trust as a denial mechanism to protect their clients, members of the communities hosted on their platforms, because cyber criminals negatively affect user stickiness and thus revenues. Jyh-Jeng Wu and Alex S. L. Tsang, in their article "Factors Affecting Members' Trust Belief and Behavior Intention in Virtual Communities," (2008), describe measures used by providers, in addition to establishing a reputation system, to build trust: clearly stating and effectively enforcing rules and regulations; monitoring members' behavior; and providing conflict resolution mechanisms.

The cases of eBay and Blizzard Entertainment show how these trust-building mechanisms are used. EBay created a Trust and Safety Team whose responsibility is to keep its virtual marketplace safe by fostering "trust between members through the development and enforcement of rules and policies, the creation of reputation-building programs, and the prevention of fraud, [and proactively working] with law enforcement and government agencies throughout the world." On the other hand, Blizzard Entertainment, a top online gaming company, has a series of guidelines and rules that explain how members are expected to behave within its forums. Essentially, access to the forum is a privilege, not a right, and as such they reserve the right to suspend it for deviant behavior.

By stating rules and regulations, system providers establish a code of conduct under which members assess each other. And, by enforcing the rules and providing resolution mechanisms, they are ensuring that there is control instead of anarchy. In addition, monitoring members' behavior allows providers to take preventive actions against cyber crime and minimize the impact of any attack to the community. System providers work together with their users, internet service providers and law enforcement to create a deterrence coalition against cyber criminals.

CONCLUSION

Cyberspace has a veil of anonymity, making reputation the most precious asset in virtual communities. Cyberspace is a reflection of humanity. Individuals behave the same way when operating in cyberspace as they do in the physical realm.

People create virtual communities that are far from anarchical, with rules, duties and benefits, and their members are subject to a strong hierarchy. The systems that host virtual communities also require trust and seek to build reputation. For system providers, the relationship between reputation and reliability is exactly the same as it is for individuals. A reliable system allows access when required, clearly states the rules and effectively enforces them, monitors members' behavior and provides conflict resolution mechanisms.

Trust, through reputation building, has the potential to be widely used as a denial mechanism against cyber crime. Moreover, providers are constantly evolving to deter cyber criminals and this evolution requires active relationships with virtual community members and law enforcement. □